〈翻訳文〉

発送番号：9-5-2006-012238536
発送日付：2006.02.28
提出期日：2006.04.30

Your Ref.: NEC03P012-SIb
Our Ref.: P04251-WAK
出願番号：10-2004-7016292

特許庁

意見提出通知書

出願人　氏名　日本電気株式会社(出願人コード：519980958731)
　　住所　日本国東京都港区芝5丁目7番1号
代理人　氏名　崔達龍
　　住所　ソウル江南区駅三洞823-1豊林ビル5階
　　(崔達龍国際特許法律事務所)
出願番号　10-2004-7016292
発明の名称　ハンドオーバ制御方法

この出願に対する審査結果、下記のような拒絶理由があり特許法第63条の規定によりこれを通知しますので、意見があったり補正が必要な場合には上記の提出期日までに意見書［特許法施行規則別紙第25号の2書式］または/及び補正書［特許法施行規則別紙第5号書式］を提出して下さい。(上記の提出期日に対して毎回1ヶ月単位で延長を申請することができ、この申請に対して別途の期間延長承認の通知はしません。)

【理由】

1. この出願は特許請求範囲第25項及び第26項は‘･･･プログラム’を請求していますが、これは装置と方法の発明のうちどの範疇にも属さないもので、発明のカテゴリが明確でないため特許法第42条第4項第2号の規定による要件を満たすことができずにいます。

2. この出願の特許請求範囲第1項乃至第5項、第9項乃至第13項、第17項乃至第21項、第25項及び第26項に記載された発明は、その出願前にこの発明が属する技術分野で通常の知識を有した者(以下‘当業者’という)が下記に指摘したことにより容易に発明することができるものであるため、特許法第29条第2項の規定により特許を受けることができません。

【下記】

▶引用発明1→国際公開特許公報WO 2001/39538号(2001.05.31)
：移動端末機の要求により既存接続APはSAデータベースから保安連係パラメータを検索して結果が含まれたハンドオーバー要請を移動端末機がハンドオーバーされた新しいAPに伝送して認証することを特徴とする移動端末機ハンドオーバーの間保安連係の伝送

▶引用発明2→国内公開特許公報第2001-78772号(2001.08.21)
：移動端末機の認証のために第1基地局で一つまたは二つ以上の保安情報セットを第2

基地局に伝送することを特徴とする無線通信で安全なハンドオフを容易にする方法

本願発明の請求範囲において、

イ.本願発明請求範囲第1項及び第3項に記載された発明は無線端末が接続する無線基地局を変更するハンドオーバー線に該当無線端末に接続されている場合に該当無線端末がハンドオーバー後に接続される他の無線基地局に該当無線端末との通信に必要な通信コンテキストを伝送する伝送手段を複数の無線基地局それぞれに有することを特徴とする無線アクセス通信システムに関する発明です。

本願発明と引用発明を対比してみると、本願発明の上記特徴は本願発明の上記特徴は引用発明1に記載された移動端末機のハンドオーバー要求によるメッセージを受信した既存接続APはSAデータベースから保安連係パラメータを検索して保安連係パラメータが含まれたハンドオーバー要請を移動端末機がハンドオーバーされる新しいAPに伝送し、認証を経てハンドオーバーされる特徴と類似します。

但し、本願発明はコンテキストを伝送するという点では差異がありますが、これは引用発明1の認証のための保安連係パラメータをコンテキスト単純変更した程度のものです。

よって、本願発明は当業者であれば引用発明1から容易に発明することができる程度のもので、その目的及び作用効果においても同一な範疇内にあるものです。

ロ.本願発明請求範囲第2項、第4項及び第5項は通信コンテキスト無線端末に関する種別が異なる複数のサブコンテキスト識別子とサブコンテキスト情報で構成されたコンテキスト情報とコンテキスト情報識別子で構成され、旧APと新規AP間に1対1及び1対多数のうちの一方に伝送されることを特徴として本願発明を限定していますが、これは引用発明2に記載された移動端末機の認証のために第1基地局から第2基地局に伝送する一つまたは二つ以上の保安情報セットの特徴と類似します。

ハ.本願発明請求範囲第9項乃至第13項、第17項乃至第21項、第25項及び第26項に記載された発明は本願発明請求範囲第1項乃至第5項に記載された無線アクセス通信システムを具現するのに必要な伝送手段を含む無線基地局、ハンドオーバー制御方法及びこれをコンピュータで実行させるためのプログラムを記録した記録媒体に関する発明で、これは本願発明の無線アクセス通信システムを具現するために当業者が自明に採択することができる事項で、上記拒絶理由‘2－イ’及び‘2－ロ’の理由と同一な理由でその技術上の特異性が認められません。

【添付】

添付1 WO2001039538 1部。

添付2 国内公開特許公報第2001-78772号(2001.08.21) 1部。以上。

2006.02.28

발송번호: 9-5-2006-012238536
발송일자: 2006.02.28
제출기일: 2006.04.30

수신 서울 강남구 역삼동 823-1 풍림빌딩 5층
(최달용국제특허법률사무소)
최달용

135-080

특 허 청
의견제출통지서

출원인 명칭 닛본 덴끼 가부시끼가이샤 (출원인코드: 519980958731)
주소 일본국 도꾜도 미나도꾸 시바 5쪼메 7방 1고
대리인 명칭 최달용
주소 서울 강남구 역삼동 823-1 풍림빌딩
5층(최달용국제특허법률사무소)

출원번호 10-2004-7016292
발명의 명칭 핸드오버 제어 방법

이 출원에 대한 심사결과 아래와 같은 거절이유가 있어 특허법 제63조의 규정에 의하여 이를 통지하오니 의견이 있거나 보정이 필요할 경우에는 상기 제출기일까지 의견서[특허법시행규칙 별지 제25호의2서식] 또는/및 보정서[특허법시행규칙 별지 제5호서식]를 제출하여 주시기 바랍니다.(상기 제출기일에 대하여 매회 1월 단위로 연장을 신청할 수 있으며, 이 신청에 대하여 별도의 기간연장승인통지는 하지 않습니다.)

[이유]

1. 이 출원은 특허청구범위 제25항 및 제26항은 '…프로그램' 을 청구하고 있으나, 이는 장치와 방법의 발명중 어느 범주에도 속하지 않는 것으로 발명의 카테고리가 명확하지 않아서 특허법제42조제4항제2호의 규정에 의한 요건을 충족하지 못하고 있습니다.

2. 이 출원의 특허청구범위 제1항 내지 제5항, 제9항 내지 제13항, 제17항 내지 제21항, 제25항 및 제26항에 기재된 발명은 그 출원전에 이 발명이 속하는 기술분야에서 통상의 지식을 가진 자(이하 '당업자'라 함)가 아래에 지적한 것에 의하여 용이하게 발명할 수 있는 것이므로 특허법 제29조제2항의 규정에 의하여 특허를 받을 수 없습니다.

[아래]

▶ 인용발명1 → 국제공개특허공보 WO 2001/39538호(2001.05.31)
: 이동단말기의 요구에 의해 기존 접속 AP는 SA 데이터베이스로부터 보안연계 파라미터를 검색하여 결과가 포함된 핸드오버 요청을 이동 단말기가 핸드오버될 새로운 AP로 전송하여 인증하는 것을 특징으로 하는 이동 단말기 핸드오버동안 보안 연계의 전송

▶ 인용발명2 → 국내공개특허공보 제2001-78772호(2001.08.21)
: 이동 단말기의 인증을 위해 제1 기지국에서 하나 또는 둘이상의 보안 정보세트를 제2기지국으로 전송하는 것을 특징으로 하는 무선 통신에서 안전한 핸드오프를 용이하게 하는 방법

본원발명의 청구범위에 있어서,

가. 본원발명 청구범위 제1항 및 제3항에 기재된 발명은 무선 단말이 접속하는 무선 기지국을 변경하는 핸드오버 전에 해당 무선 단말에 접속되어 있는 경우에 해당 무선 단말이 핸드오버 후에 접속되는 다른 무선 기지국에 해당 무선 단말과의 통신에 필요한 통신 콘텍스트를 전송하는 전송 수단을 복수의 무선 기지국 각각에 갖는 것을 특징으로 하는 무선 액세스 통신 시스템에 관한 발명입니다.

본원발명과 인용발명을 대비해 보면, 본원발명의 상기 특징은 인용발명1에 기재된 이동단말기의 핸드오버 요구에 의한 메시지를 수신한 기존 접속 AP는 SA데이터베이스로부터 보안연계 파라미터를 검색하여 보안연계 파라미터가 포함된 핸드오버 요청을 이동단말기가 핸드오버될 새로운 AP로 전송하고, 인증을 거쳐 핸드오버 되는 특징과 유사합니다.

다만, 본원발명은 콘텍스트를 전송한다고 하는 점에서는 차이가 있으나, 이는 인용발명1의 인증을 위한 보안연계 파라미터를 콘텍스트로 단순 변경한 정도의 것입니다.

따라서, 본원발명은 당업자라면 인용발명1로부터 용이하게 발명할 수 있는 정도의 것으로서, 그 목적 및 작용효과에 있어서도 동일한 범주내에 있는 것입니다.

나. 본원발명 청구범위 제2항, 제4항 및 제5항은 통신 콘텍스트는 무선 단말에 관한 종별이 다른 복수의 서브콘텍스트 식별자와 서브콘텍스트 정보로 구성된 콘텍스트 정보와 콘텍스트 정보 식별자로 구성되어, 구AP와 신규AP간에 1 대 1 및 1 대 다수 중의 한쪽으로 전송되는 것을 특징으로 하여 본원발명을 한정하고 있으나, 이는 인용발명2에 기재된 이동 단말기의 인증을 위해 제1 기지국에서 제2기지국으로 전송하는 하나 또는 둘이상의 보안 정보세트의 특징과 유사합니다.

다. 본원발명 청구범위 제9항 내지 제13항, 제17항 내지 제21항, 제25항 및 제26항에 기재된 발명은 본원발명 청구범위 제1항 내지 제5항에 기재된 무선 액세스 통신 시스템을 구현하는데 필요한 전송 수단을 포함하는 무선기지국, 핸드오버 제어방법 및 이를 컴퓨터에서 실행시키기 위한 프로그램을 기록한 기록 매체에 관한 발명으로서, 이는 본원발명의 무선 액세스 통신 시스템을 구현하기 위해 당업자가 자명하게 채택할 수 있는 사항으로 상기 거절이유 '2-가' 및 '2-나'의 이유와 동일한 이유로 그 기술상의 특이성이 인정되지 않습니다.

[첨 부]

첨부1 WO2001039538호 1부.

첨부2 국내공개특허공보 제2001-78772호(2001.08.21) 1부. 끝.

2006.02.28

특허청 전기전자심사본부

정보심사팀 심사관 김병균

심사관 김병우

<< 안내 >>

명세서 또는 도면 등의 보정서를 전자문서로 제출할 경우 매건 3,000원, 서면으로 제출할 경우 매건 13,000원의 보정료를 납부하여야 합니다.

보정료는 접수번호를 부여받아 이를 납부자번호로 "특허법·실용신안법·디자인보호법및상표법에 의한 특허료·등록료와 수수료의 징수규칙" 별지 제1호서식에 기재하여, 접수번호를 부여받은 날의 다음 날까지 납부하여야 합니다. 다만, 납부일이 공휴일(토요휴무일을 포함한다)에 해당하는 경우에는 그날 이후의 첫 번째 근무일까지 납부하여야 합니다.

보정료는 국고수납은행(대부분의 시중은행)에 납부하거나, 인터넷지로(www.giro.go.kr)로 납부할 수 있습니다. 다만, 보정서를 우편으로 제출하는 경우에는 보정료에 상응하는 통상환을 동봉하여 제출하시면 특허청에서 납부해드립니다.

기타 문의사항이 있으시면 ☎042)481-8300로 문의하시기 바랍니다.

서식 또는 절차에 대하여는 특허고객 콜센터(☎1544-8080)로 문의하시기 바랍니다.

Your Ref.: NEC03P012-SIb
Our Ref.: P04251-WAK
出願番号：10-2004-7016292

韓国公開特許公報第2001-78772号

【特許請求の範囲】
【請求項1】
少なくとも第1、2無線基地局と少なくとも一つの無線移動端末機を有するネットワークで安全なハンドオフを容易にする方法において、
上記第1基地局から上記第2基地局までハンドオフに対して上記少なくとも一つの無線移動端末機から要求を受信する段階、
上記要求に応答して上記第1基地局から上記第2基地局まで保安情報を伝送する段階を含む安全なハンドオフを容易にする方法。

【請求項9】
少なくとも第1、第2無線基地局と一つの無線端末機を有する無線通信サービスを提供するネットワークでハンドオフを遂行する方法において、
上記第1基地局から上記第2基地局までハンドオフに対する上記無線端末機から要求を伝送する段階、
上記第2基地局が上記第1基地局と容易なハンドオフをすることができると指示する上記要求を受信する前に上記第2基地局が上記第1基地局がわかっているとき、上記無線端末機に応答を受信する段階、
ユーザー通信用上記無線端末機を上記第2基地局に接続する段階を含むハンドオフの遂行方法。

【請求項17】
少なくとも第1、第2無線基地局と少なくとも一つの無線端末機を有するネットワークでハンドオフを遂行する方法において、
ハンドオフ用上記無線端末機から上記第1基地局を経て上記第2基地局まで要求を伝送する段階、
上記要求を受信する前に上記第2基地局が上記第1基地局がわかっていないとき、上記第1基地局から供給された情報の利益なしに上記第2基地局に連結しなければならないという指示を上記無線端末機で受信する段階を含むハンドオフの遂行方法。

【請求項21】

少なくとも第1、第2基地局と少なくとも一つの無線端末機を有するネットワークでハンドオフを遂行する方法において、

ハンドオフ用上記無線端末機から上記第1基地局を経て上記第2基地局まで上記第2基地局により要求を受信する段階、

上記要求を受信する前に上記第2基地局が上記第1基地局がわかっているとき、促進されたハンドオフを遂行する段階、

上記要求を遂行する前に第2基地局が上記第1基地局がわからないとき、非促進されたハンドオフを遂行する段階を含むハンドオフの遂行方法。

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04B 7/26

(11) 공개번호 특2001-0078772
(43) 공개일자 2001년08월21일

(21) 출원번호 10-2001-0005534
(22) 출원일자 2001년02월06일
(30) 우선권주장 09/501,168 2000년02월09일 미국(US)
(71) 출원인 루센트 테크놀러지스 인크
미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자 데이비스스티븐윌리엄
캐나다엠5에스2에이치9토론토아파트먼트2스파디나애비뉴661
반더빈미카엘라씨
미국뉴저지주07738린크로프트윌로우그로브드라이브114
(74) 대리인 김창세, 장성구

심사청구 : 없음

(54) 무선 통신에서 안전한 핸드오프를 용이하게 하는 방법

요약

네트워크에 규정된 경계를 기지국 수준까지 하방으로 밀어낸다. 그렇게 하는 것은 무선 단말기가 통신을 스위칭할 때마다 인증을 필요로 하거나 또는 한 기지국에서 다른 기지국까지 '핸드오프'를 필요로 한다. 이러한 인증을 효율적인 방식으로 수행하기 위해서, 보안 정보, 즉, 유도된 정보가 한 기지국으로부터 다른 기지국까지 직접 전송된다. '직접'이란, 기지국에 대한 상호접속 경로를 형성하는 네트워크의 다른 간섭 노드를 거쳐 정보가 전송될지라도, '유도된 정보의 다른 소스에 접속하지 않고'를 의미한다. 단순화된 네트워크, 즉, 제어 관점으로 볼 때 축소된 계층을 갖는 네트워크, 예컨대, 상호 접속부와 함께 단지 홈 위치 레지스터 및 기지국 네트워크 장치를 요구하는 네트워크가 핸드오프 과정 동안에 성능은 최소로 감소하고, 예컨대 지연은 최소로 증가하도록 이용될 수 있다. 본 발명의 한 실시예에 있어서, 무선 단말기로부터 최초로 서비스 요구를 수신하는 제 1 기지국은 중앙 보안 노드로부터 인증 정보를 요구하고, 응답으로 적어도 하나, 통상 2 이상의 보안 정보 세트를 수신한다. 제 1 기지국으로부터 제 2 기지국까지 핸드오프할 시간이 되었을 때, 제 1 기지국은 중앙 보안 노드로부터 수신한 적어도 하나의 보안 정보 세트를 제 2 기지국으로 전송한다. 그 후, 제 2 기지국은 제 1 기지국으로부터 수신한 정보를 사용하여 무선 단말기를 인증한다.

대표도

도2

명세서

도면의 간단한 설명

도 1은 본 발명의 원리에 따른 전형적인 네트워크 구성을 도시한 도면,

도 2는 본 발명의 원리에 따른 도 1의 기지국간의 핸드오프를 수행하는 전형적인 과정을 도시한 흐름도.

도면의 주요 부분에 대한 부호의 설명

101 : 무선 단말기 103 : 기지국

105 : 안테나 107 : 구조체

109 : 셀(cell) 111 : 네트워크

113 : 기지국 인증 유닛 115, 117, 121 : 통신 링크

119 : 보안 센터

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

본 발명은 무선 통신 기술에 관한 것으로서, 특히, 무선 통신 서비스를 제공하는 네트워크의 정당한 사용자만이 네트워크에 접속할 수 있는 것을 보장하는 시스템에 관한 것이다.

종래의 무선 시스템은 무선 네트워크에 접속하기 위해 단지 정당한 무선 단말기만을 허용한다. 네트워크에 무선 단말기 접속을 허용하기 위해서, 무선 단말기는 인증(authentication)을 받아야 한다. '인증'이라는 용어는 여기에서 종래의 방식으로, 예컨대 어떤 사람이라고 주장하는 존재가 진정으로 그 사람인지를 증명하는 과정으로 사용된다. 통화하는 동안, 예컨대 본래는 통화가 시작될 때 그리고 그 후 무선 단말기가 네트워크의 임의의 규정된 경계를 가로질러 천이할 때마다, 인증이 여러번 필요할 수 있다.

무선 단말기내에 저장된 비밀 정보로부터 유도된 정보(derived information)와 네트워크내의 다른 곳에 존재하는 동일한 유도된 정보를 비교함으로써 인증이 달성된다. 통상적으로, 비교 위치에 '가장 가까운' 유도된 정보의 저장 위치로부터 단일 통화하는 동안, 특정 무선 단말기에 대해 새로운 인증이 요구될 때마다 유도된 정보가 전송되어야 한다. 여기에서, '가장 가까운'이란 네트워크 계층(network hierarchy)의 관점에서 말하는 것이다.

무선 단말기는 에어링크(airlink)를 거쳐 기지국과 통신한다. 기지국이 비교 위치가 아니라면, 기지국은 무선 단말기로부터 비교에 사용하기 위한 비교 위치로 정보를 전송해야 한다. 유도된 정보가 저장된 네트워크내의 위치는 통상적으로 소위 '방문객 위치 레지스터(visitor location resister; VLR)'내에 있다. 유도된 정보는 네트워크내의 소위 '홈 위치 레지스터(home location resister; HLR)' 또는 특정 네트워크 설계에 따라 존재할 수도 있는 다른 인증 센터에 발생된다. 무선 단말기가 제 1 VLR에 의해 제공된 영역을 제 2 VLR에 의해 제공된 영역으로 분리하는 네트워크 경계를 교차(cross)할 때, 제 1 VLR는 유도된 정보를 그 사용을 위해 제 2 VLR로 전송할 수 있다. 한편, 제 2 VLR는 HLR로부터 그 자신의 유도된 정보를 얻을 수 있다. HLR에 의해 직접 제공된 영역에서 무선 단말기가 먼저 파워-업(power up)될 때 HLR은 VLR과 같이 작용할 수 있음을 유의하여야 한다.

바람직하지 못하게, 다양한 특정의 장치들 및 복합 제어 과정들이 필요하기 때문에, 종래 기술의 네트워크의 비용은 고가(高價)이다.

발명이 이루고자 하는 기술적 과제

우리는 네트워크내에 규정된 경계를 기지국 수준까지 하방으로 밀어냄으로써, 네트워크 구조를 단순화할 수 있고, 네트워크 설치에 관련한 비용을 감축할 수 있다는 사실은 알고 있다. 그러나, 그 결과는 무선 단말기가 한 기지국으로부터 다른 기지국으로 통신을 전환(switching)할 때마다 인증이 요구된다는 것이다. 다시 말해서, 규정된 경계를 기지국 수준까지 하방으로 밀어낸 후, 한 기지국으로부터 다른 기지국까지 무선 단말기의 핸드오프가 있을 때마다 네트워크 경계가 교차되고 인증이 요구된다. 효율적인 방식으로 이러한 인증을 달성하기 위해서, 본 발명의 원리에 따라, 보안 정보(security information), 즉 유도된 정보가 한 기지국으로부터 다른 기지국으로 직접 전송된다. '직접'이란 기지국용 상호접속 경로를 형성하는 네트워크의 다른 간섭 노드(intervening nodes)를 거쳐 정보가 전송될 수 있을 지라도, 유도된 정보의 임의의 다른 소스(source)에 접속하지 않는 것을 의미한다. 바람직하게는, 단순화된 네트워크, 즉 제어 관점으로부터 볼 때 축소된 계층을 갖는 네트워크, 예컨대 단지 HLR 및 상호접속부와 함께 기지국 네트워크 장치를 요구하는 네트워크는 핸드오프 과정 동안, 성능은 약간 감소하고, 예컨대 지연(delay)은 약간 증가하는 상태로 이용될 수 있다.

발명의 구성 및 작용

보다 구체적으로, 본 발명의 한 실시예에 있어서, 무선 단말기로부터 서비스 요구를 최초로 수신하는 제 1 기지국은 중앙 보안 노드(central security node), 즉 HLR로부터 인증 정보를 요구하고, 응답으로 적어도 하나, 통상 2 이상의 보안 정보 세트(set)를 수신한다. 보안 정보 세트는 패스워드(password), 질문-응답 쌍(challenge-reaponse pair), 질문-응답 암호 키 한 벌(challenge-reaponse cipher key turple) 등일 수 있다. 제 1 기지국으로부터 제 2 기지국까지 핸드오프할 시간일 때, 제 1 기지국은 중앙 보안 노드로부터 수신한 보안 정보 세트 중 적어도 하나를 제 2 기지국으로 전송한다. 그 후, 제 2 기지국은 제 1 기지국으로부터 수신한 정보를 사용하여 무선 단말기를 인증하고/인증하거나 암호화된 통신에 관여한다.

후술하는 바는 단지 본 발명의 원리에 대해 설명하는 것이다. 그러므로 여기에서 명백히 설명하거나 도시되지 않았더라도, 당업자라면 본 발명의 원리를 구현하며 본 발명의 정신 및 범위내에 포함된 다양한 구성을 고안할 수 있다고 이해되어야 한다. 더욱이, 여기에서 인용된 모든 예와 조건부적인 언어는 주로, 단지 교육적인 목적으로 본 발명의 원리 및 발명자(들)에 의한 기술 발전에 공헌한 개념을 이해하는데 있어서 독자를 돕고자 한 것이고, 이러한 구체적으로 인용된 예와 조건에 한정되지 않는 것으로 해석된다. 또한, 그 특정예 뿐만 아니라 본 발명의 원리, 특징, 실시예를 인용한 모든 문구는 그 구조적 및 기능적 균등물을 포함하고자 한다. 부가적으로, 이러한 균등물은 미래에 개발된 균등물, 즉 구조에 관계없이 동일한 기능을 수행하는 개발된 요소 뿐만 아니라 현재 알려진 균등물 모두를 포함하고자 한다.

그러므로, 예컨대, 당업자라면 여기의 블록도는 본 발명의 원리를 구현하는 도식적 회로에 대한 개념도를 나타낸다고 이해할 것이다. 마찬가지로, 임의의 흐름도(flow charts), 플로우 다이아그램(flow diagrams), 상태 천이도(state transition diagram), 의사코드(pseudocode) 등은 컴퓨터 판독가능 매체에 실질적으로 표현될 수 있고 그에 따라 컴퓨터 또는 프로세서(processor)가 명백히 도시되었는지 여부에

상관없이 컴퓨터 또는 프로세서에 의해 실행될 수 있는 다양한 과정(processes)을 나타낸다고 이해될 것이다.

'프로세서'라고 표시된 기능적인 블럭을 포함하여 도면에 도시된 다양한 요소의 기능들은 적절한 소프트웨어와 관련하여 소프트웨어를 실행할 수 있는 하드웨어 뿐만 아니라 전용 하드웨어(dedicated hardware)를 사용하여 제공될 수 있다. 프로세서에 의해 제공될 때, 단일 전용 프로세서(single dedicated processor), 단일 공유 프로세서(single shared processor) 또는 그들 중 몇몇이 공유될 수 있는 복수의 개개의 프로세서에 의해 이러한 기능이 제공될 수 있다. 더욱이, '프로세서' 또는 '콘트롤러(controller)' 용어의 명백한 사용은 오로지 소프트웨어를 실행할 수 있는 하드웨어에 사용되는 것으로 해석되서는 안되고, 제한 없이, 디지털 신호 프로세서(digital signal processor; DSP) 하드웨어, 저장 소프트웨어용 판독 전용 기억 장치(read-only memory; ROM), 임의 접근 기억 장치(random access memory; RAM) 및 비휘발성 저장부(non-volatile storage)를 함축적으로 포함할 수 있다. 종래의 하드웨어 및/또는 주문형(custom) 하드웨어 등의 다른 하드웨어가 또한 포함될 수 있다. 마찬가지로, 도면에 도시된 임의의 스위치는 단지 개념적인 것이다. 그 기능은 프로그램 로직(program logic)의 동작, 전용 로직, 프로그램 제어와 전용 로직의 상호작용을 통하여 또는 심지어 수동으로 수행될 수 있고, 특정 기술은 문맥으로부터 보다 구체적으로 이해되는 바와 같이 구현자에 의해 선택가능하다.

본 발명의 청구 범위에 있어서, 특정 기능을 수행하는 수단으로서 표현되는 임의의 요소는, 예컨대 1) 그 기능을 수행하는 회로 소자의 조합 또는 2) 소프트웨어를 실행하여 그 기능을 수행하는 적절한 회로로 조합된, 펌웨어(firmware), 마이크로코드(microcode) 등을 포함하는 임의의 형태의 소프트웨어를 포함하는 기능을 수행하는 임의의 방법을 포함하고자 한다. 이러한 청구 범위에 의해 규정된 발명은 다양한 인용 수단에 의해 제공되는 기능성(functionalities)이 청구 범위가 요구하는 방식으로 조합되고 수집된다는 사실에 있다. 그러므로, 출원인은 이러한 기능성을 제공할 수 있는 임의의 수단을 여기에 도시된 수단의 균등물로 생각한다.

다만 여기에서 명백하게 구체화되지 않은 것은 도면에 정확한 축적으로 도시되어 있지 않다.

도 1은 본 발명의 원리에 따른 전형적인 네트워크 구성을 도시하고 있다. 도 1에는 1) 무선 단말기(101), 2) 기지국(103-1) 내지 기지국(103-N)을 포함하는 N 기지국(103), 여기서 N은 2이상의 정수, 3) 안테나(105-1) 내지 안테나(105-N)를 포함하는 N 안테나(105), 4) 구조체(107-1) 내지 구조체(107-N)를 포함하는 N 구조체(107), 5) 셀(109-1) 내지 셀(109-N)을 포함하는 N 셀(109), 6) 네트워크(111), 7) 기지국 인증 유닛(113), 8) 통신 링크(115-1) 내지 통신 링크(115-N)을 포함하는 N 통신 링크(115), 9) 통신 링크(117) 및 (121), 10)보안 센터(119)가 도시되어 있다.

무선 단말기(101)는 무선 단말기(101)의 현재 위치에서 통신하기 위해 검출되고 사용가능하도록 충분한 신호 강도로 전송하는 다수의 기지국들과 통신할 수 있다. 일단 충분한 강도의 신호가 특정 기지국에 검출되면, 무선 단말기(101)는 그 기지국과의 통신에 관여할 수 있다. 무선 단말기(101)에 의해 이용되는 무선 링크 및 프로토콜(protocol)의 특정 유형(type), 즉 에어 인터페이스(air interface)는 본 발명에 필수적이지 않고, 물론 무선 단말기(101)에 의해 이용되는 라디오 링크(radio link) 및 프로토콜은 기지국(103)에 의해 이용되는 것과 동일한 유형이어야 한다고 하더라도, 구현자가 원하는 임의의 유형일 수 있다.

무선 단말기(101)는 구현자가 원하는 임의의 방식으로 다수의 기지국과 통신할 수 있다. 예컨대, 무선 단말기(101)는 단지 하나의 수신기를 가질 수 있고, 그 수신기는 현재 정보를 제공하는 기지국과의 정보의 교환으로 점유되지 않을 때, 무선 단말기(101)에 도달하는 충분한 강도의 신호를 갖는 다른 기지국으로부터 신호를 수신할 수 있다. 한편, 무선 단말기(101)는 동시에 다수의 기지국으로부터, 예컨대 무선 단말기(101)내의 다수의 병렬 수신기를 이용함으로써 신호를 수신할 수 있다. 한편, 무선 단말기(101)는 2 이상의 수신기를 가질 수 있다. 그러나 수신기의 수는 무선 단말기(101)가 그의 현재 위치에서 충분한 강도의 신호를 수신할 수 있는 기지국의 수보다 적다. 그래서, 무선 단말기(101)는 적어도 하나의 수신기에 주사(scanning)를 수행하여 몇몇의 기지국에 대한 신호를 얻을 필요가 있다.

기지국(103)은 후술하는 것을 제외하고 실질적으로 종래의 기지국이다. 첫째, 기지국(103)은 기지국간 통신 전용 네트워크에 접속될 필요가 없다. 대신에, 기지국(103)은 공유된 공중망(public network), 예컨대 인터넷(Internet) 등의 인터넷 프로토콜(IP)-계 네트워크를 이용할 수 있다. 둘째, 각 기지국(103)은 임의의 '맵(map)' 정보를 포함할 필요가 없다. 대신에, 각각의 기지국(103)은 '맵' 정보의 필요한 부분을 발견할 수 있다. 바람직하게는, 기지국(103)은 전용 구조 및 사이트 준비(site preparation)를 요구하기 보다 오히려, 작은 공간, 예컨대 이미 이용가능한 공간 속에 용이하게 포함될 수 있는 소형 기지국이다. 바람직하게는, '맵' 정보의 필요한 부분을 발견하는 능력이 결합된 이러한 소형은 새로운 무선 통신 네트워크의 빠른 구축을 가능하게 한다. 더욱이, 이러한 무선 통신 네트워크는 그 구성에 있어서 융통성이 있다. 즉, 기지국이 용이하게 첨가되거나 제거될 수 있고, 또한 유지하기가 용이하다.

각각의 안테나(105)는 기지국(103)중 하나에 결합된다. 각각의 안테나(105)는 기지국(103)중 하나에 의해 발생된 신호를 방사한다. 기지국(103) 중 하나와 안테나(105)중 하나를 조합하여 특정 포괄 영역인 셀(109)중 하나를 만든다. 도 1의 셀(109)의 형상은 실제 셀 형상을 나타낸 것이 아니라, 단지 셀에 대한 종래의 표시일 뿐이다. 실제 다양한 셀(109)의 형상은 모두 독립적이라는 것에 유의해야 한다.

각각의 구조체(107)는 하나 이상의 기지국(103)의 설치를 용이하게 한다. 더욱이, 구조체(107)는 또한 안테나(105)를 탑재할 장소를 제공할 수 있다. 예컨대, 구조체(107)중 몇몇은 기지국(103)중 하나가 미사용된 공간에 위치하고 안테나(105)중 하나가 외부에 부착된 이미 존재하고 있는 집(homes)일 수 있다.

네트워크(111)는 기지국(103)에 대한 통로(way)를 제공하여, 기지국 인증 유닛(113) 및 보안 센터(119)와의 통신 뿐만 아니라 기지국 상호간에 통신을 가능하게 한다. 네트워크(111)는 그 자체만으로 네트워크일 수 있는 다양한 서브네트워크(subnetwork)로 구성될 수 있다. 더욱이, 이 다양한 서스네트워크들은 다른 유형일 수 있고, 다른 프로토콜을 이용할 수 있다. 본 발명의 한 실시예에 있어서, 네트워크(111)는 패킷 형식 네트워크(packet based network), 예컨대 비동기 전송 모드(asynchronous transfer mode; ATM) 네트

워크 또는 IP 네트워크이다.

각각의 기지국(103)은 네트워크(111)의 일부라고 할 수 있는 개개의 통신 링크(115)중 하나를 거쳐 네트워크(111)에 접속된다. 예컨대, 네트워크(111), 또는 적어도 그의 서브네트워크가 IP 네트워크이고, 기지국(103)중 하나가 집인 구조체(107)내에 위치하는 곳에, 통신 링크(115)는, 예컨대 다른 가지국과의 통신을 위한 기지국에 의해 그리고 인터넷 브라우징(browsing)을 하기 위한 집의 점유자에 의해 공유되는 케이블 텔레비전 선 또는 파이버-커브 접속부(fiber-to-curb connection)를 넘어서 인터넷 접속부일 수 있다.

기지국 인증 유닛(113)은 모든 유효한 기지국(103)의 리스트(list)와 보안 키 및 선택적인 신원 확인자 또는 기지국의 주소 등의 임의의 관련 정보를 포함한다. 기지국은 임의의 지점에서 기지국 인증 유닛(113)에 나와 있을 수 있다. 그러나, 기지국은 단지 그것이 기지국 인증 유닛(113)에 나와 있을 때 유효하게 된다. 여기에서는 단일 유닛으로서 도시될 지라도, 실제로 기지국 인증 유닛(113)은 지리적으로 함께 둘 필요가 없는 수개의 부분들(parts)로 구성될 수 있다. 더욱이, 신뢰도 및 성능을 향상시키기 위해서, 당업자에 의해 용이하게 인식되는 바와 같이, 기지국 인증 유닛(113)의 몇몇의 또는 모든 다양한 부분 또는 기능이 복제될 수 있다.

기지국 인증 유닛(113)은 통신 링크(117)를 거쳐 네트워크(111)에 접속된다. 물론, 기지국 인증 유닛(113)이 2 이상의 부분으로 구성되거나 또는 복제될 때, 통신 링크(117)는 네트워크(111)와 다양한 부분 또는 복제물 사이의 모든 필요한 통신 경로를 포괄하는 것으로 해석된다.

보안 센터(119)는 제공될 수 있는 모든 유효한 무선 단말기의 리스트를 포함한다. 또한, 보안 센터(119)는 인증 질문-응답 쌍 및/또는 각 무선 단말기와 관련한 암호 키 등의 보안 정보를 포함한다. 보안 정보는 필요할 때 보안 센터(119)에 의해 기지국(103)으로 분배될 수 있다. 무선 단말기는 임의의 지점에서 보안 센터(119)에 기록될 수 있다. 그러나, 무선 단말기는 단지 그것이 보안 센터(119)에 기록될 때 유효하게 된다. 여기에서는 단일 유닛으로 도시될 지라도, 실제로 보안 센터(119)는 지리적으로 함께 둘 필요가 없는 수개의 부분들로 구성될 수 있다. 더욱이, 신뢰도 및 성능을 향상시키기 위해서, 당업자에 의해 용이하게 인식되는 바와 같이, 보안 센터(119)의 몇몇의 또는 모든 다양한 부분 또는 기능이 복제될 수 있다.

보안 센터(119)는 통신 링크(121)를 거쳐 네트워크(111)에 접속된다. 물론, 보안 센터(119)가 2 이상의 부분으로 구성되거나 또는 복제될 때, 통신 링크(121)는 네트워크(111)과 다양한 부분 또는 복제물 사이의 모든 필요한 통신 경로를 포괄하는 것으로 해석된다.

도 2는 본 발명의 원리에 따라 도 1의 기지국들 사이에 핸드오프를 수행하는 전형적인 과정을 도시한 흐름도이다. 보다 구체적으로, 핸드오프 과정의 일부로서, 기지국은 기지국의 '맵' 중 적어도 일부분, 즉, 존재한다면, 인접한 기지국의 패턴(pattern) 및 관련 정보를 발견할 수 있고 업데이트(update)할 수 있다. 예컨대, 여기에 완전히 기재된 것처럼 참고로 구현된 우리의 동시 출원된 미국 특허 출원 순차 번호(사건 데이비스(Davies) I-5)를 참조해야 한다. 특정 기지국에 의해 발견된 맵의 부분은 통상적으로 기지국이 제공하고 있는 통화를 핸드오프할 수 있는 인접 기지국이다. 특정 기지국이 그의 완전한 국부적인 맵을 발견하는 데에는 각각의 이러한 인접 기지국을 갖는 적어도 하나의 핸드오프가 필요하다.

통신하고 있는 기지국, 예컨대 기지국(103-1)(도 1)의 라디오 링크 신호가 다른 특정 기지국, 예컨대 기지국(103-2)의 라디오 링크 신호보다 충분히 약하게 되기 때문에, 무선 단말기, 예컨대 무선 단말기(101)(도 1)가 핸드오프를 요구하여, 다른 특정 기지국이 더 양호한 라디오 링크를 제공할 수 있었던 것으로 보이는 것이 결정될 때, 단계(201)로 과정이 시작된다. 다음의 조건 분기점(203)(도 2)은 제 1 기지국으로부터 수신된 신호가 무선 단말기에서 약하게 되거나, 또는 무선 단말기로부터 나와 제 1 기지국에서 수신된 신호가 약하게 되어, 핸드오프가 달성되기 전에 제 1 기지국과 무선 단말기 사이의 접속이 끊기는 것이 가능하기 때문에, 제 1 기지국, 예컨대 도 1의 기지국 103-1에 대한 접속이 여전히 존재하는지 여부를 결정하는 시험을 한다. 단계(203)에서의 시험 결과가 YES라면, 제 1 기지국과 무선 단말기 사이의 접속이 계속해서 존재하는 것을 나타내어, 단계(205)로 보내지고, 단계(205)에서는 무선 단말기가 제 1 기지국으로부터 제 2 기지국, 예컨대 도 1의 기지국(103-2)으로 핸드오프를 요구한다. 한편, 무선 단말기는 제 1, 제 2 기지국에 대해 무선 단말기에서 수신된 신호 강도의 다양한 측정을 제 1 기지국으로 보낼 수 있고, 제 1 기지국은 핸드오프하기에 적당한 시간인지를 결정한다. 그러므로, 제 1 기지국은 무선 단말기에게 제 2 기지국과 접속하라고 명령한다.

다음으로, 조건 분기점(207)은 제 1 기지국이 제 2 기지국을 '알고 있는지' 여부, 즉 제 1 기지국의 '맵' 정보에 제 2 기지국이 기록되어 있는지 여부를 결정하는 시험을 한다. 이러한 기록은 제 1 기지국과 제 2 기지국 사이의 무선 단말기의 종전의 핸드오프의 결과였다. 보다 구체적으로, 맵 정보내의 기록의 일부로서, 제 1 기지국은 1) 제 2 기지국의 기지국 확인, 2) 제 2 기지국의 네트워크 주소, 예컨대 그의 IP 주소, 3) 본 발명의 한 측면에 따라, 제 1 기지국과 제 2 기지국 사이의 안전한 통신에 사용되는 제 2 기지국의 공중 키 등의 보안 정보를 알 수 있다. 단계(207)의 시험 결과가 NO라면, 제 1 기지국이 제 2 기지국을 알고 있지 않다고 나타내어, 단계(209)로 보내진다. 단계(209)에서 제 1 기지국은 무선 단말기에게 제 2 기지국을 알고 있지 않으며 무선 단말기는 그 자체로 제 2 기지국과 무선 링크 접속을 위해 배열되어야 한다고 명령한다. 이것은, 예컨대 후술하는 바와 같이, 무선 단말기가 기지국에 의해 제공된 셀내에서 먼저 파워-업될 때 기지국과의 최초의 무선 링크를 설정하기 위해서 무선 단말기가 사용하는 동일한 과정을 사용함으로써 달성될 수 있다.

단계(203)의 시험 결과가 NO라면, 무선 단말기로부터 제 1 기지국으로의 접속이 종료에 이르렀음을 나타내거나, 또는 단계(209) 후에, 단계(211)로 보내진다. 단계(211)에서 무선 단말기는 제 2 기지국이 무선 단말기에 무선 링크를 설정하도록 요구한다. 이러한 요구에 응답하여, 조건 분기점(212)에 있어서, 제 2 기지국은 그것이 제 1 기지국을 알고 있는지 여부를 결정하는 시험을 한다. 단계(212)의 시험 결과가 NO라면, 제 2 기지국이 제 1 기지국을 알고 있지 않다고 나타내어, 단계(213)으로 보내진다. 단계(203)에서는 제 2 기지국이 보안 센터, 예컨대 도 1의 보안 센터(119)에 저장된 정보의 협의(consultation)를 통상적으로 요구하는 무선 단말기를 인증하는 것을 시도한다. 그 후에, 단계(215)로 보내지고, 이 과정은 후

술하는 바와 같이 계속된다. 단계(212)의 시험 결과가 YES라면, 단계(214)로 보내지고, 단계(214)에서는, 본 발명의 원리에 따라, 무선 단말기에 대한 제 1 기지국의 보안 정보가 제 2 기지국에 의해 요구되고, 제 1 기지국으로부터 수신된다. 바람직하게는, 이미 제 1 기지국을 신뢰하는 제 2 기지국은 보안 센터로 무선 단말기의 인증에 관여할 필요가 없으며, 그에 따라 상당한 시간을 절약할 수 있고 핸드오프 과정을 용이하게 할 수 있다. 약간 특별한 상황이라고 생각되기 때문에 도 2에 도시되어 있지 않더라도, 제 1 기지국에 이용가능한 보안 정보가 없는 경우, 예컨대 제 1 기지국에 이용가능한 모든 보안 정보가 이미 고갈된 경우에, 단계(213)으로 보내어야 한다.

단계(207)의 시험 결과가 YES라면, 제 1 기지국이 제 2 기지국을 알고 있다고 나타내어, 조건 분기점(208)로 보내진다. 조건 분기점(208)에서는 제 1 기지국이, 본 발명의 원리에 따라, 제 2 기지국에 의해 사용될 수 있는 무선 단말기에 대해 이용가능한 보안 정보를 가지고 있는지 여부를 결정하는 시험을 한다. 이러한 보안 정보는 질문-응답 인증 쌍 및/또는 무선 단말기에 관련한 암호화 키 등일 수 있다. 단계(208)의 시험 결과가 NO라면, 제 1 기지국은 제 2 기지국에 의해 사용될 수 있는 무선 단말기에 대해 이용가능한 어떠한 보안 정보도 가지고 있지 않다고 나타내어, 단계(209)로 보내지고, 이 과정은 후술하는 바와 같이 계속된다. 단계(208)의 시험 결과가 YES라면, 제 1 기지국이 제 2 기지국에 의해 사용될 수 있는 무선 단말기에 대해 이용가능한 보안 정보를 가지고 있다고 나타내어 단계(221)로 보내진다. 단계(221)에서는 본 발명의 원리에 따라, 제 1 기지국이, 예컨대 자발적으로, 이용가능한 보안 정보를 제 2 기지국으로 보낸다. 이러한 보안 정보의 전송은 제 2 기지국에서 제 1 기지국으로부터 제 2 기지국으로의 무선 단말기의 핸드오프에 대한 요구로 해석될 수 있다. 바람직하게는, 이미 제 1 기지국을 신뢰하는 제 2 기지국은 보안 센터로 무선 단말기의 인증에 관여할 필요가 없으며, 그러므로 상당한 시간을 절약할 수 있고 핸드오프 과정을 용이하게 할 수 있다.

다음으로, 단계(223)에 있어서, 무선 단말기는 제 2 기지국이 무선 단말기에 무선 링크를 설정하도록 요구한다. 그 후에, 또는 단계(214)의 실행 후에, 조건 분기점)(225)로 보내지고, 조건 분기점(225)은 무선 단말기가 암호를 사용하여 제 1 기지국과 그 데이터를 통신하고 있었는지 여부를 결정하는 시험을 한다. 단계(225)의 시험 결과가 NO라면, 암호화되지 않은 링크가 무선 단말기에 의해 사용되어 제 1 기지국과 그 데이터를 통신하고 있었음을 나타내어 단계(227)로 보내진다. 단계(227)에서는, 제 2 기지국이 제 1 기지국으로부터 얻은 보안 정보를 사용하여 무선 단말기를 인증한다.

그 후에, 조건 분기점(215)은 무선 단말기가 성공적으로 인증되었는가를 결정하는 시험을 한다. 단계(215)의 시험 결과가 YES라면, 무선 단말기가 통신하기 위해 기지국을 이용하게 됨을 나타내어, 단계(231)로 보내지고, 단계(231)에서는, 무선 단말기가 사용자 통신량을 운송하기 위해 제 2 기지국에 접속된다. 그 후에, 과정은 단계(233)에서 종료된다. 단계(215)의 시험 결과가 NO라면, 무선 단말기가 통신하기 위해 기지국을 이용하지 못하게 됨을 나타내어, 단계(233)으로 보내지고, 과정은 종료된다.

단계(225)의 시험 결과가 YES라면, 암호화된 링크가 무선 단말기에 의해 사용되어 기지국과 그 데이터를 통신하고 있었음을 나타내어, 단계(229)로 보내지고, 단계(229)에서는 데이터 처리의 암호화 및 해독이 무선 단말기와 제 2 기지국 사이에서 시작된다. 이러한 목적으로 암호화 알고리즘(ciphering algorithm)의 초기치가 설정된다. 사용자 데이터가 흘러나오면, 그것은 자동적으로 적절히 암호화되거나 또는 해독된다. 무선 단말기가 무선 단말기를 수신하기 위해 촉진된 핸드오프에 참여하지 않은 기지국의 셀내에서 인증받고 활성화된 후에, 제 1 기지국으로부터 제 2 기지국으로 통과된 새로운 암호화 키를 갖는 암호화된 링크의 사용은 무선 단말기의 직접적인 재인증(reauthentication)으로서 동일한 목적을 달성한다는 것을 유의해야 한다.

그 후, 단계(231)로 보내지고, 단계(231)에서는, 무선 단말기가 사용자 통신량을 운송하기 위해 제 2 기지국에 접속된다. 또한, 이 단계의 일부로서 데이터를 제 1 기지국을 거쳐 무선 단말기로 전송하고 있었던 네트워크의 다른 부분은, 예컨대 잘 알려진 이동 인터넷 프로토콜(Mobile Internet Protocol)의 기술을 사용하여, 이제 데이터를 제 2 기지국을 거쳐 무선 단말기로 전송하도록 지시받는다. 그 후, 과정은 단계(233)에서 종료된다.

단계(207)의 YES 결과는 마찬가지로 제 2 기지국이 제 1 기지국을 알고 있음을 의미하며, 이것은 단지 특수한 에러(error)의 경우에는 적용되지 않을 것임을 유의해야 한다. 촉진된 핸드오프에 참여하기 위해 제 2 기지국의 거절(refusal)에 의해 지시될 이러한 에러는, 예컨대 단계(209)로 보내져서 촉진되지 않은 핸드오프를 수행하는 과정을 요구한다.

또한, 제 1 기지국은 그것이 최초로 수신한 모든 보안 정보를 제 2 기지국으로 보낼 수 없다는 것을 유의해야 한다. 이에 대한 한가지 이유는 제 1 기지국이 무선 단말기와 통신함에 있어서 그 정보의 일정량을 사용하였기 때문이다. 그리고, 임의의 보안 공격을 막기 위해서, 질문-응답 쌍 또는 암호화 키 등의 보안 정보의 소정의 유형을 단 한번 사용하는 것은 좋은 방법이다. 더욱이, 제 1 기지국에 의해 얻어진 보안 정보가 보안 센터 또는 다른 기지국으로부터 얻을 수 있다는 것을 유의해야 한다.

발명의 효과

본 발명의 원리에 따라, 보안 정보, 즉 유도된 정보를 한 기지국으로부터 다른 기지국으로 직접 전송하여 인증을 효율적으로 달성하고, 핸드오프 과정 동안 성능은 최소로 감소하며, 지연은 최소로 증가한다.

(57) 청구의 범위

청구항 1

적어도 제 1, 제 2 무선 기지국과 적어도 하나의 무선 이동 단말기를 갖는 네트워크에서 안전한 핸드오프를 용이하게 하는 방법에 있어서,

상기 제 1 기지국으로부터 상기 제 2 기지국까지 핸드오프에 대해 상기 적어도 하나의 무선 이동 단말기

로부터 요구를 수신하는 단계,

상기 요구에 응답하여 상기 제 1 기지국으로부터 상기 제 2 기지국까지 보안 정보를 전송하는 단계

를 포함하는 안전한 핸드오프를 용이하게 하는 방법.

청구항 2

제 1 항에 있어서,

상기 보안 정보는 적어도 난수를 포함하는 세트, 상기 제 1 또는 제 2 기지국이 아닌 상기 무선 이동 단말기에 의해 유도될 수 있는 증명자 및 키를 포함하는 안전한 핸드오프를 용이하게 하는 방법.

청구항 3

제 1 항에 있어서,

적어도 상기 보안 정보의 일부분은 상기 제 2 기지국에 대해 상기 적어도 하나의 이동 무선 단말기를 유효하게 하는데 사용되는 안전한 핸드오프를 용이하게 하는 방법.

청구항 4

제 1 항에 있어서,

상기 요구에 응답하여 상기 제 1 기지국으로부터 제 2 기지국으로 전송된 상기 보안 정보는 상기 제 1 기지국에 의해 수신된 모든 보안 정보보다 적은 안전한 핸드오프를 용이하게 하는 방법.

청구항 5

제 4 항에 있어서,

상기 제 1 기지국에 의해 수신된 모든 보안 정보는 무선 이동 단말기 유효화 시스템으로부터 수신되었던 안전한 핸드오프를 용이하게 하는 방법.

청구항 6

제 4 항에 있어서,

상기 제 1 기지국에 의해 수신된 모든 보안 정보는 제 3 기지국으로부터 수신되었던 안전한 핸드오프를 용이하게 하는 방법.

청구항 7

제 1 항에 있어서,

상기 수신하는 단계 전에 상기 제 1 기지국이 상기 제 2 기지국을 알고 있을 때에만 상기 요구에 응답하여 상기 제 1 기지국으로부터 상기 제 2 기지국으로 보안 정보가 전송되는 안전한 핸드오프를 용이하게 하는 방법.

청구항 8

제 1 항에 있어서,

상기 제 1 기지국과 상기 무선 단말기가 암호화된 링크를 사용하여 통신하고 있을 때 상기 제 2 기지국과 상기 무선 단말기 사이의 암호화된 링크를 시작하는 단계를 더 포함하되,

상기 제 2 기지국과 상기 무선 단말기 사이에 상기 암호화된 링크를 시작하는데 있어서, 상기 제 2 기지국은 상기 제 1 기지국으로부터 상기 제 2 기지국까지 전송된 상기 보안 정보를 사용하는 안전한 핸드오프를 용이하게 하는 방법.

청구항 9

적어도 제 1, 제 2 무선 기지국과 적어도 하나의 무선 단말기를 갖는 무선 통신 서비스를 제공하는 네트워크에서 핸드오프를 수행하는 방법에 있어서,

상기 제 1 기지국으로부터 상기 제 2 기지국까지 핸드오프에 대한 상기 무선 단말기로부터 요구를 전송하는 단계,

상기 제 2 기지국이 상기 제 1 기지국과 용이한 핸드오프를 할 수 있다고 지시하는 상기 요구를 수신하기

전에 상기 제 2 기지국이 상기 제 1기지국을 알고 있을 때, 상기 무선 단말기에 응답을 수신하는 단계,

사용자 통신용 상기 무선 단말기를 상기 제 2 기지구에 접속하는 단계

를 포함하는 핸드오프의 수행 방법.

청구항 10

제 9 항에 있어서,

상기 응이한 핸드오프는 상기 제 1 기지국으로부터 제 2 기지국까지 전송된 상기 무선 단말기에 대한 정보를 이용하는 핸드오프의 수행 방법.

청구항 11

제 10 항에 있어서,

상기 정보는 보안 정보인 핸드오프의 수행 방법.

청구항 12

제 10 항에 있어서,

상기 정보는 보안 센터으로부터 수신된 보안 정보인 핸드오프의 수행 방법.

청구항 13

제 10 항에 있어서,

상기 정보는 상기 제 1 또는 제 2 기지국 이외의 기지국으로부터 수신된 보안 정보인 핸드오프의 수행 방법.

청구항 14

제 10 항에 있어서,

상기 정보는 보안 정보이고, (1) 패스워드, (2) 질문-응답 쌍, (3) 질문-응답 암호 키 한 벌로 구성된 세트로부터 적어도 하나를 포함하는 핸드오프의 수행 방법.

청구항 15

제 10 항에 있어서,

상기 정보는 기지국간 통신용 네트워크에 대해서 수신된 보안 정보인 핸드오프의 수행 방법.

청구항 16

제 10 항에 있어서,

상기 접속하는 단계는 상기 핸드오프 요구 전에 상기 제 1 기지국과 상기 무선 단말기가 암호화된 링크를 사용하여 통신하고 있을 때 상기 제 2 기지국과 상기 무선 단말기 사이의 암호화된 링크를 시작하는 단계를 더 포함하되,

상기 제 2 기지국과 상기 무선 단말기 사이에 상기 암호화된 링크를 시작하는데 있어서, 상기 제 2 기지국은 상기 응답의 일부로서 상기 제 1 기지국으로부터 상기 제 2 기지국까지 전송된 상기 보안 정보를 사용하는 핸드오프의 수행 방법.

청구항 17

적어도 제 1, 제 2 무선 기지국과 적어도 하나의 무선 단말기를 갖는 네트워크에서 핸드오프를 수행하는 방법에 있어서,

핸드오프용 상기 무선 단말기로부터 상기 제 1 기지국을 거쳐 상기 제 2 기지국가지 요구를 전송하는 단계,

상기 요구를 수신하기 전에 상기 제 2 기지국이 상기 제 1 기지국을 알고 있지 않을 때, 상기 제 1 기지국으로부터 공급된 정보의 이익 없이 상기 제 2 기지국에 연결하여야 한다는 지시를 상기 무선 단말기에서 수신하는 단계

를 포함하는 핸드오프의 수행 방법.

청구항 18

제 17 항에 있어서,

상기 정보는 보안 정보인 핸드오프의 수행 방법.

청구항 19

제 17 항에 있어서,

상기 정보는 보안 센터로부터 수신된 보안 정보인 핸드오프의 수행 방법.

청구항 20

제 17 항에 있어서,

상기 정보는 상기 제 1 또는 제 2 기지국 이외의 기지국으로부터 수신된 보안 정보인 핸드오프의 수행 방법.

청구항 21

적어도 제 1, 제 2 기지국과 적어도 하나의 무선 단말기를 갖는 네트워크에서 핸드오프를 수행하는 방법에 있어서,

핸드오프용 상기 무선 단말기로부터 상기 제 1 기지국을 거쳐 상기 제 2 기지국까지 상기 제 2 기지국에 의해 요구를 수신하는 단계,

상기 요구를 수신하기 전에 상기 제 2 기지국이 상기 제 1 기지국을 알고 있을 때, 촉진된 핸드오프를 수행하는 단계,

상기 요구를 수신하기 전에 제 2 기지국이 상기 제 1 기지국을 알지 못할 때, 비촉진된 핸드오프를 수행하는 단계

를 포함하는 핸드 오프의 수행 방법.

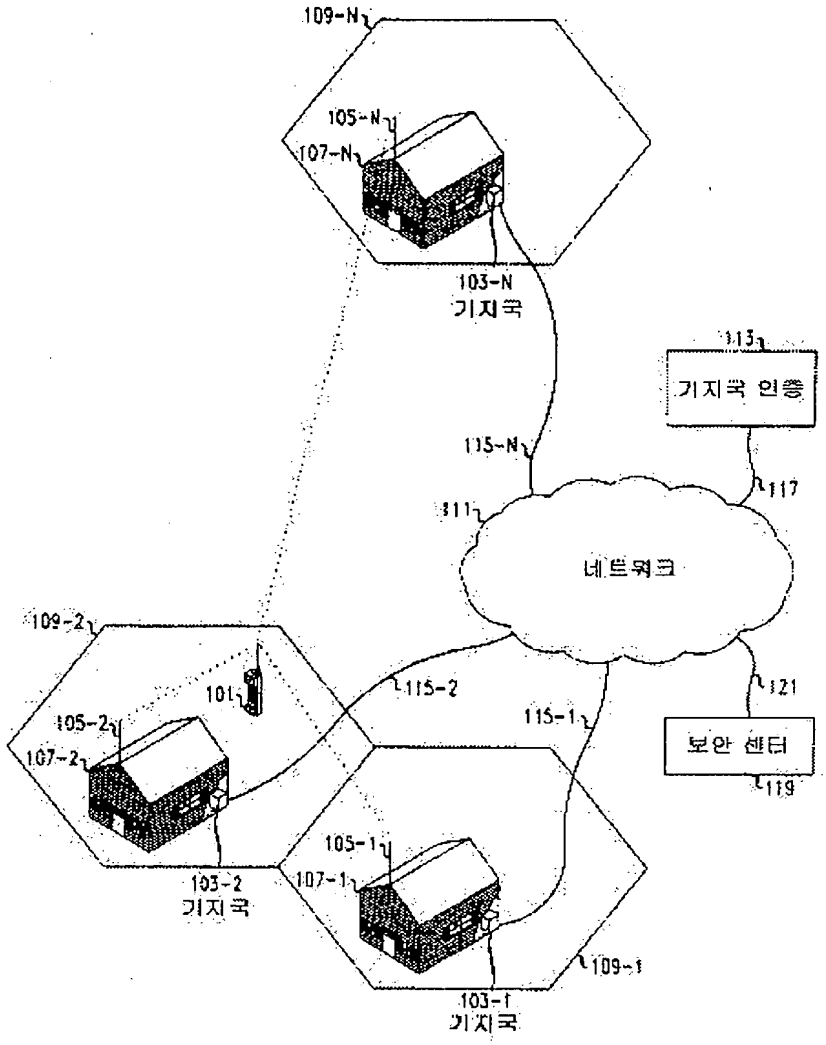
청구항 22

제 21 항에 있어서,

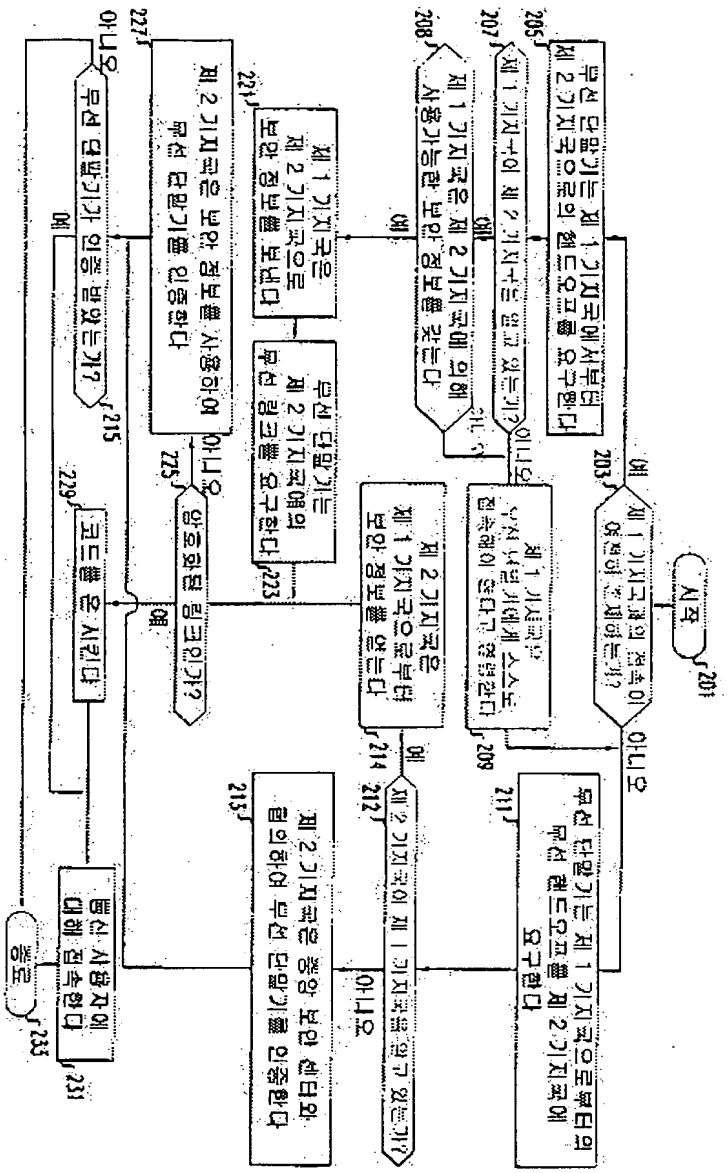
상기 촉진된 핸드오프를 수행하는 단계는 상기 제 1 기지국으로부터 상기 제 2 기지국까지 보안 정보를 전송하는 단계를 포함하는 핸드 오프의 수행 방법.

도면

도면1


109-N
105-N
107-N
103-N
기지국
113
기지국 인증
115-N
117
111
네트워크
109-2
101
105-2
107-2
115-2
115-1
121
보안 센터
119
105-1
107-1
103-2
기지국
109-1
103-1
기지국

도면2


시작
201
제 1 기지국과의 접속이 요청되었는가?
203
예
아니오
무선 단말기는 제 1 기지국에서부터 제 2 기지국으로의 핸드오프를 요구한다
205
제 1 기지국은 제 2 기지국에 의해 사용가능한 보안 정보를 갖는다
208
제 1 기지국은 제 2 기지국에 의해 사용가능한 보안 정보를 갖는다
208
예
제 1 기지국과의 접속이 종료되었는가?
207
아니오
제 1 기지국은 제 2 기지국에 의해 사용가능한 보안 정보를 갖는다
208
제 1 기지국은 제 2 기지국으로 보안 정보를 보낸다
221
무선 단말기는 제 2 기지국에 의해 무선 링크를 요구한다
223
제 2 기지국은 보안 정보를 사용하여 무선 단말기를 인증한다
225
암호화된 링크인가?
아니오
예
제 2 기지국은 제 1 기지국으로부터 보안 정보를 얻는다
214
제 2 기지국이 제 1 기지국을 필요로 하는가?
212
예
아니오
무선 단말기는 제 1 기지국으로부터 무선 핸드오프를 제 2 기지국에 요구한다
211
제 2 기지국은 중앙 보안 센터와 협의하여 무선 단말기를 인증한다
213
무선 단말기가 인증을 받았는가?
227
아니오
예
코드를 송신한다
229
통신 사용자에 대해 접속한다
231
종료
233